OWASP In Action:
Tools for the DISA ASD STIG

Jason Li
Principal Consultant
jason.li@aspectsecurity.com

OWASP
November 12, 2009

The OWASP Foundation
http://www.owasp.org

About Me

- Principal Consultant
- OWASP Global Projects Committee Co-Chair

ASPECT SECURITY
Application Security Specialists

About DISA

- Defense Information Systems Agency

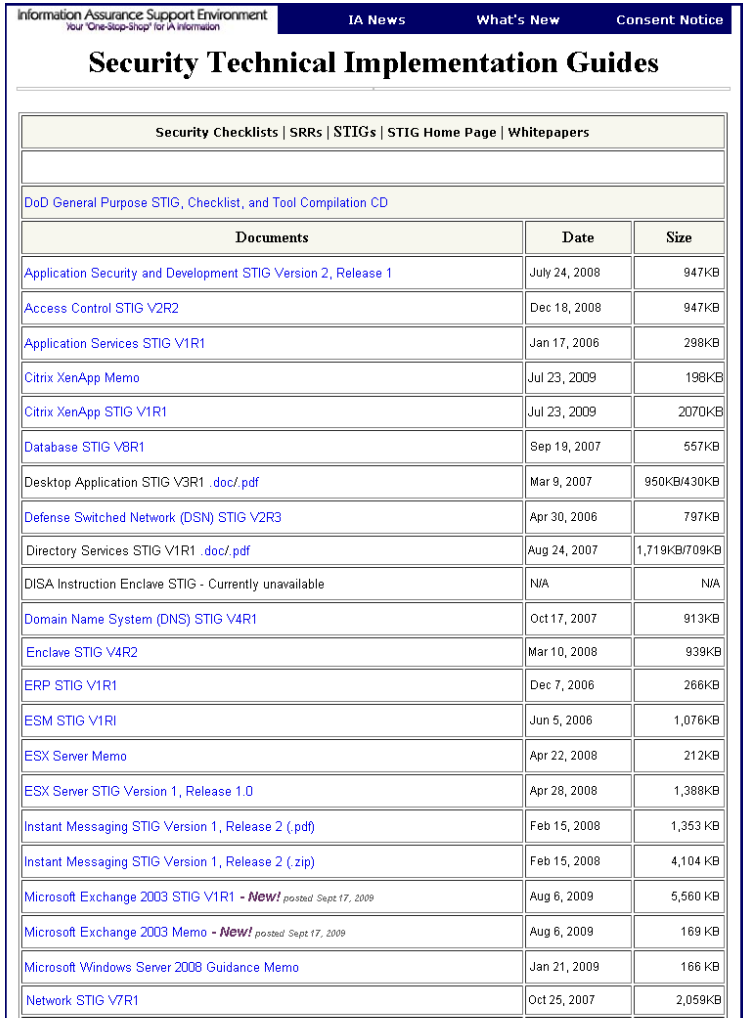
- Part of the Department of Defense

- Administers and protects DoD command and control systems and enterprise infrastructure

About DISA STIGs

- Offers configuration guides and checklists for:
  - Databases
  - Operating Systems
  - Web Servers
  - Etc…

- Provides standard "findings" and impact ratings
  - CAT I, CAT II, CAT III


Information Assurance Support Environment
Your 'One-Stop-Shop' for IA information
IA News
What's New
Consent Notice

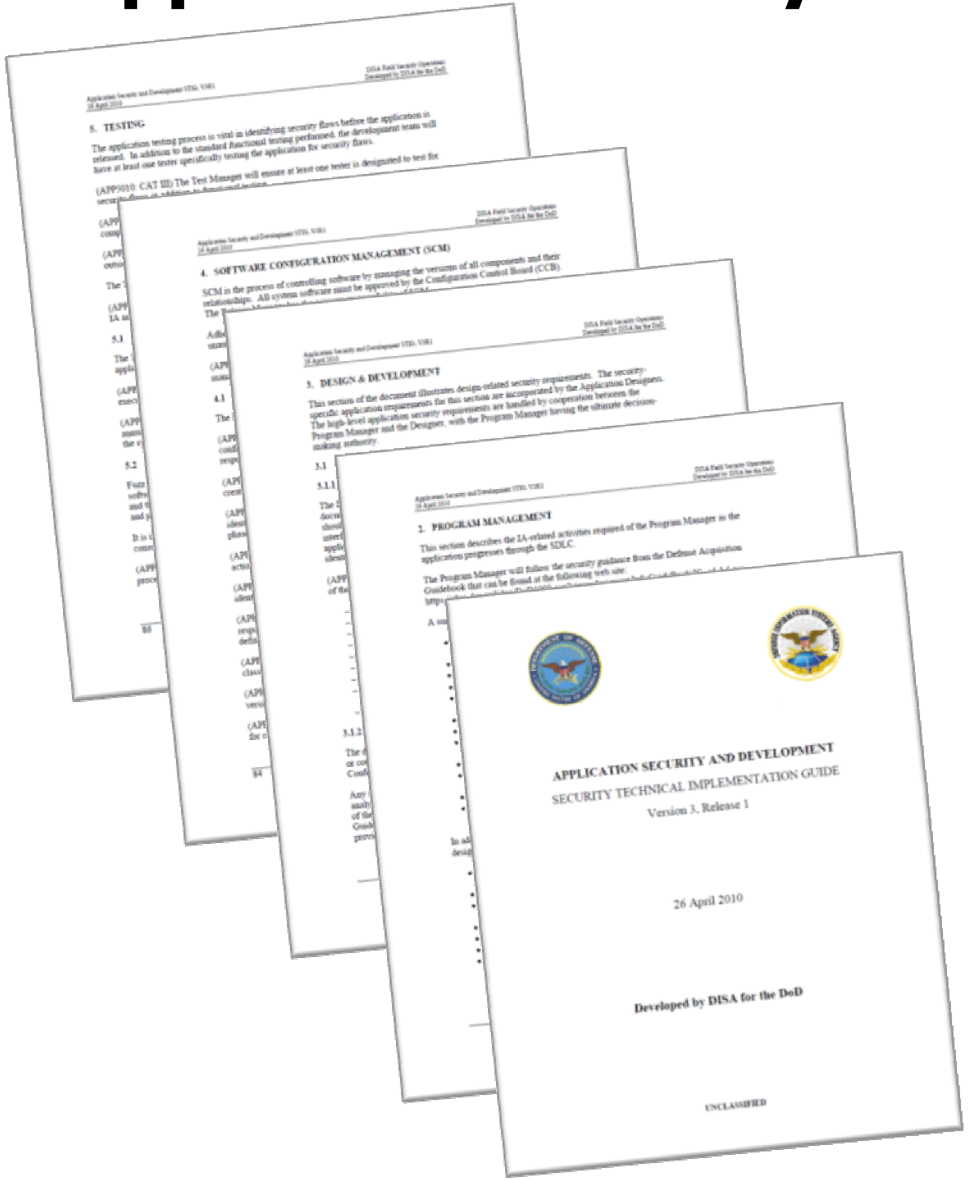
Security Technical Implementation Guides

Security Checklists | SRRs | STIGs | STIG Home Page | Whitepapers

DoD General Purpose STIG, Checklist, and Tool Compilation CD

Documents	Date	Size
Application Security and Development STIG Version 2, Release 1	July 24, 2008	947KB
Access Control STIG V2R2	Dec 18, 2008	947KB
Application Services STIG V1R1	Jan 17, 2006	298KB
Citrix XenApp Memo	Jul 23, 2009	198KB
Citrix XenApp STIG V1R1	Jul 23, 2009	2070KB
Database STIG V8R1	Sep 19, 2007	557KB
Desktop Application STIG V3R1 .doc/.pdf	Mar 9, 2007	950KB/430KB
Defense Switched Network (DSN) STIG V2R3	Apr 30, 2006	797KB
Directory Services STIG V1R1 .doc/.pdf	Aug 24, 2007	1,719KB/709KB
DISA Instruction Enclave STIG - Currently unavailable	N/A	N/A
Domain Name System (DNS) STIG V4R1	Oct 17, 2007	913KB
Enclave STIG V4R2	Mar 10, 2008	939KB
ERP STIG V1R1	Dec 7, 2006	266KB
ESM STIG V1RI	Jun 5, 2006	1,076KB
ESX Server Memo	Apr 22, 2008	212KB
ESX Server STIG Version 1, Release 1.0	Apr 28, 2008	1,388KB
Instant Messaging STIG Version 1, Release 2 (.pdf)	Feb 15, 2008	1,353 KB
Instant Messaging STIG Version 1, Release 2 (.zip)	Feb 15, 2008	4,104 KB
Microsoft Exchange 2003 STIG V1R1 - *New!* *posted Sept 17, 2009*	Aug 6, 2009	5,560 KB
Microsoft Exchange 2003 Memo - *New!* *posted Sept 17, 2009*	Aug 6, 2009	169 KB
Microsoft Windows Server 2008 Guidance Memo	Jan 21, 2009	166 KB
Network STIG V7R1	Oct 25, 2007	2,059KB

Application Security and Development STIG



APPLICATION SECURITY AND DEVELOPMENT

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 3, Release 1

26 April 2010

Developed by DISA for the DoD

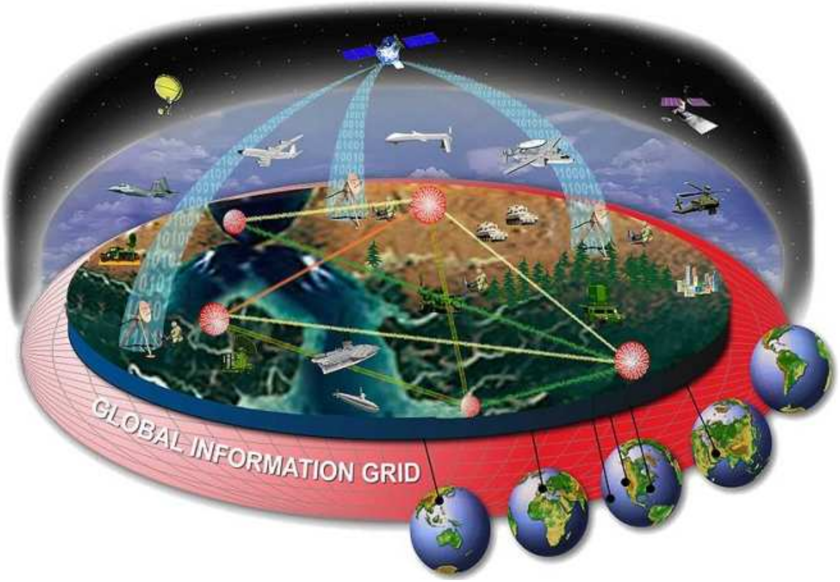
UNCLASSIFIED

- First draft Nov 2006
- First release Jul 2008
- Current release Apr 2010

- 157 requirements covering:
  - Program Management
  - Design & Development
  - Software Configuration Management
  - Testing
  - Deployment

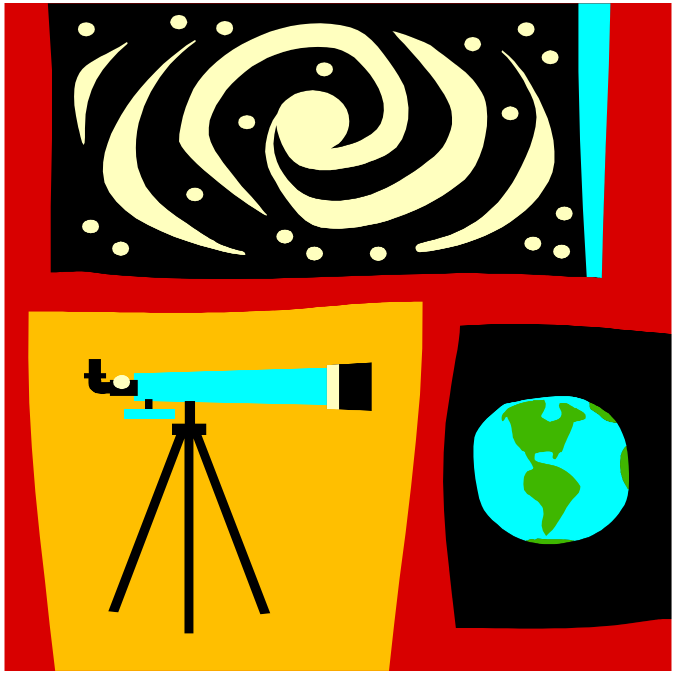
Application Security and Development STIG

- ASD STIG applies to "*all DoD developed, architected, and administered applications and systems connected to DoD networks*"
- Essentially anything plugged into DoD



Application Security and Development STIG

- Requirements can be extremely broad:
  - e.g. APP3510: The Designer will ensure the application validates all user input
  - e.g. APP3540: The Designer will ensure the application is not vulnerable to SQL Injection



Application Security and Development STIG

- Requirements can be extremely specific:
  - e.g. APP3390: The Designer will ensure users accounts are locked after three consecutive unsuccessful logon attempts within one hour

Application Security and Development STIG

- Requirements can be esoteric:
  - e.g. APP3150: The Designer will ensure the application uses FIPS 140-2 validated cryptographic modules to implement encryption, key exchange, digital signature, and hash functionality

Application Security and Development STIG

- Requirements can be expensive:
  - e.g. APP2120: The Program Manager will ensure developers are provided with training on secure design and coding practices on at least an annual basis

Lost in the Weeds

Get Organized

Types of Requirements

Procedural

- System Security Plan (APP2010)
- Incident Response Plan (APP2140)
- Registered Ports and Protocols (APP2100)

Configuration

- Disable default accounts (APP3370)
- Least Privilege Accounts (APP3500)
- Support DoD PKI certs (APP3290)

Standards

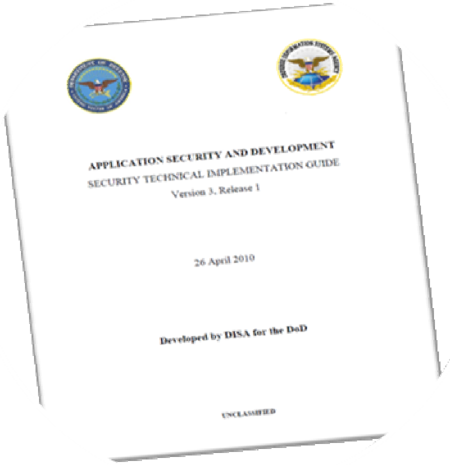
- NIAP Approved Products (APP2070)
- FIPS 140-2 Compliance (APP3150)
- NIST crypto (APP3210)

Application Security

- AppSec Training (APP2120)
- No XSS (APP3580)
- No CSRF (APP3585)
- No SQLi (APP3540)

OWASP and the ASD STIG

- OWASP is explicitly called out as a resource in the ASD STIG Checklist:
  - APP3020
  - APP3405
  - APP3570
  - APP3550
  - APP3560
  - APP3580
  - APP3810
  - APP3600
  - APP3630
  - APP5100



APPLICATION SECURITY AND DEVELOPMENT
SECURITY TECHNICAL IMPLEMENTATION GUIDE
Version 3, Release 1

26 April 2010

Developed by DISA for the DoD

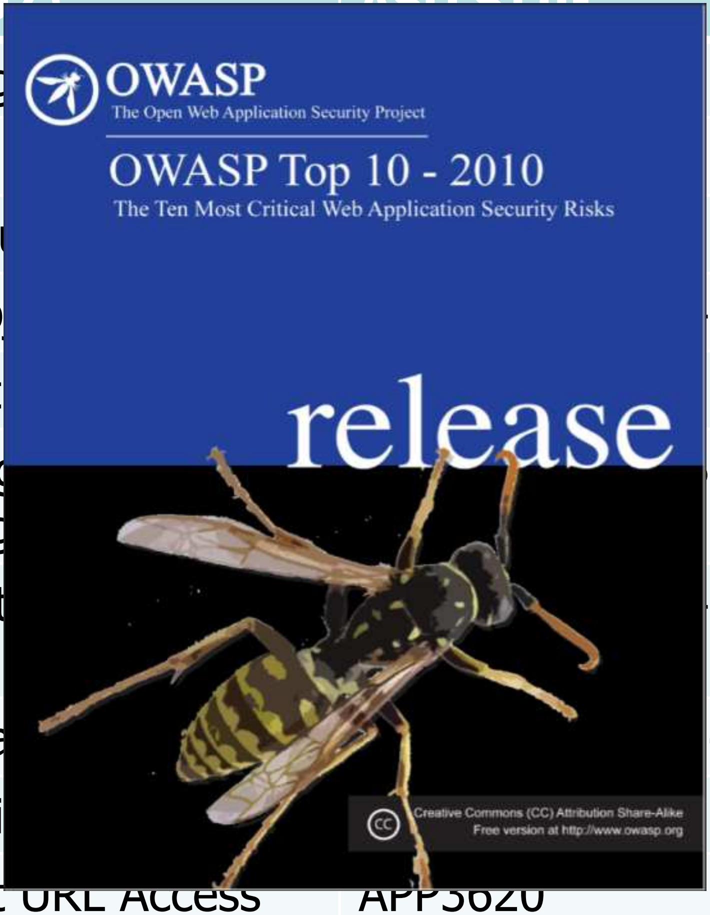
UNCLASSIFIED

OWASP Documentation Projects

OW
The Open
OW
The Ter
OWAS
The Open Web Ap
A G
Sec
App
Serv
2.0 Blac
July 27,
OWASP CODE REV
GUIDE
2008 V1.1
OWASP APP
V1.1
DETECT A
OWASP TESTING GU
2008 V3.0
OWASP
The Open Web Application Security
OWASP Appl
Verification S
– Web App
re
OWASP
The Open Web Application Security Project
SECURE SOFTWARE DEVELOPMENT
CONTRACT ANNEX
WARNING: THIS DOCUMENT SHOULD BE CONSIDERED GUIDANCE ONLY.
OWASP STRONGLY RECOMMENDS THAT YOU CONSULT A QUALIFIED
ATTORNEY TO HELP YOU NEGOTIATE A SOFTWARE CONTRACT.

OWASP Top Ten

OWASP Top Ten (2007)	ASD STIG
A1 – Cross Site Scripting	
A2 – Injection Flaws	70
A3 – Malicious File Execu	
A4 – Insecure Direct Ob	80, APP3620
A5 – Cross Site Request	
A6 – Information Leakag Improper Error Handling	20
A7 – Broken Authenticat Session Management	15, APP3420,
A8 – Insecure Cryptogra	40
A9 – Insecure Communi	30
A10 – Failure to Restrict URL Access	APP3620



OWASP

The Open Web Application Security Project

OWASP Top 10 - 2010

The Ten Most Critical Web Application Security Risks

release

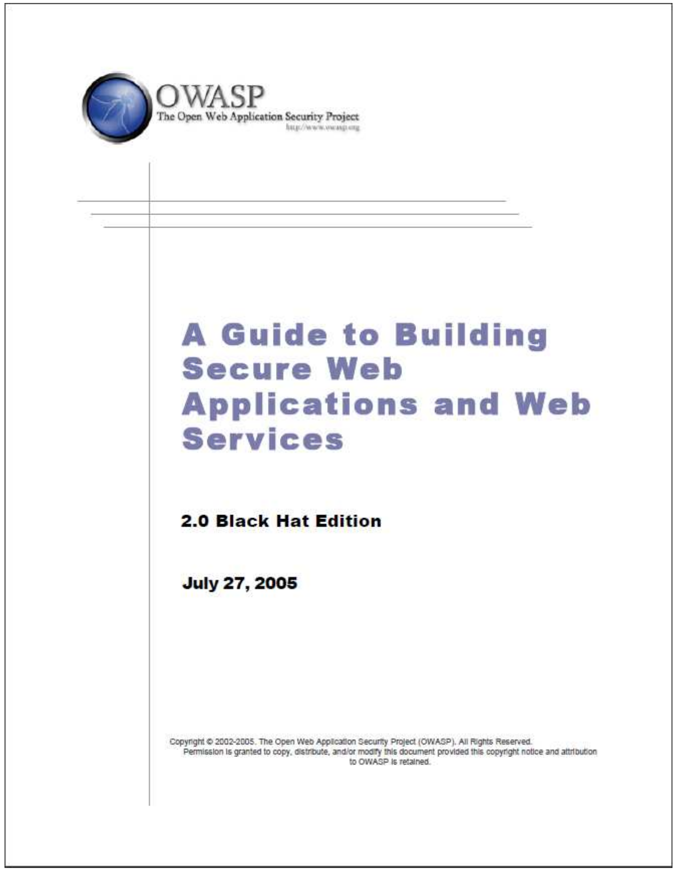
Creative Commons (CC) Attribution Share-Alike

Free version at http://www.owasp.org

APP3510 – Input Validation

- ASD STIG:
  “Ensure the application validates all input.”

- OWASP Development Guide:
  “Data Validation” chapter provides guidance to developers on how to correctly validate input



OWASP
The Open Web Application Security Project
http://www.owasp.org

A Guide to Building Secure Web Applications and Web Services

2.0 Black Hat Edition

July 27, 2005

http://www.owasp.org/index.php/Category:OWASP_Guide_Project

APP3540 – SQL Injection

- ASD STIG:
  “Ensure the application is not vulnerable to SQL Injection…”

- SQLiX Project:
  A SQL Injection scanner to crawl and detect SQL injection vectors

OWASP
SQLiX
Project

http://www.owasp.org/index.php/Category:OWASP_SQLiX_Project
(also included in the OWASP LiveCD)

APP3580 – Cross-Site Scripting

XSS
Prevention
Cheatsheet

- ASD STIG:
  "Ensure the application does not have cross site scripting (XSS) vulnerabilities."

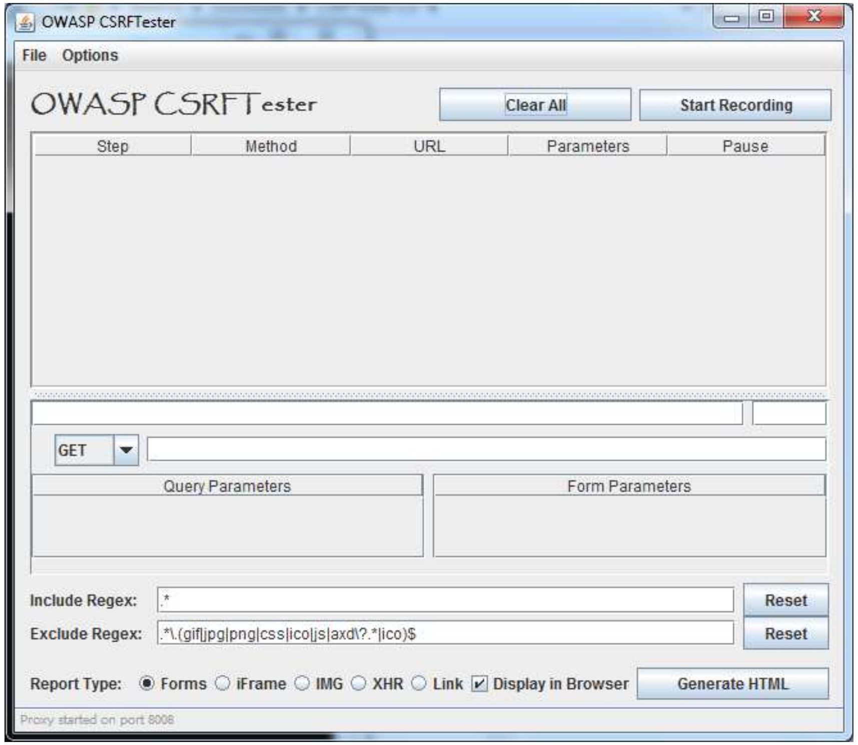
- XSS Prevention Cheatsheet:
  A simple positive model for preventing XSS using output escaping/encoding properly

http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

APP3585 – Cross-Site Request Forgery

- ASD STIG:
  Ensure the application does not have CSRF vulnerabilities.

- CSRF Tester:
  Tool that give developers the ability to test their applications for CSRF flaws



Include Regex: .*

Exclude Regex: .*\.(gif|jpg|png|css|ico|js|axd\?.*|ico)$

Report Type: ● Forms ○ iFrame ○ IMG ○ XHR ○ Link ☑ Display in Browser

Proxy started on port 8008

http://www.owasp.org/index.php/Category:OWASP_CSRFTester_Project

APP3620 – Information Disclosure

- ASD STIG:
  “Ensure the application does not disclose unnecessary information to users.”

- DirBuster Project:
  An application designed to brute force directories and files names on web/application servers.

OWASP
DirBuster
Project

http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
(also included in the OWASP LiveCD)

APP5080 – Code Review

OWASP
The Open Web Application Security Project

06/09

OWASP Application Security Verification Standard 2009

– Web Application Standard

release

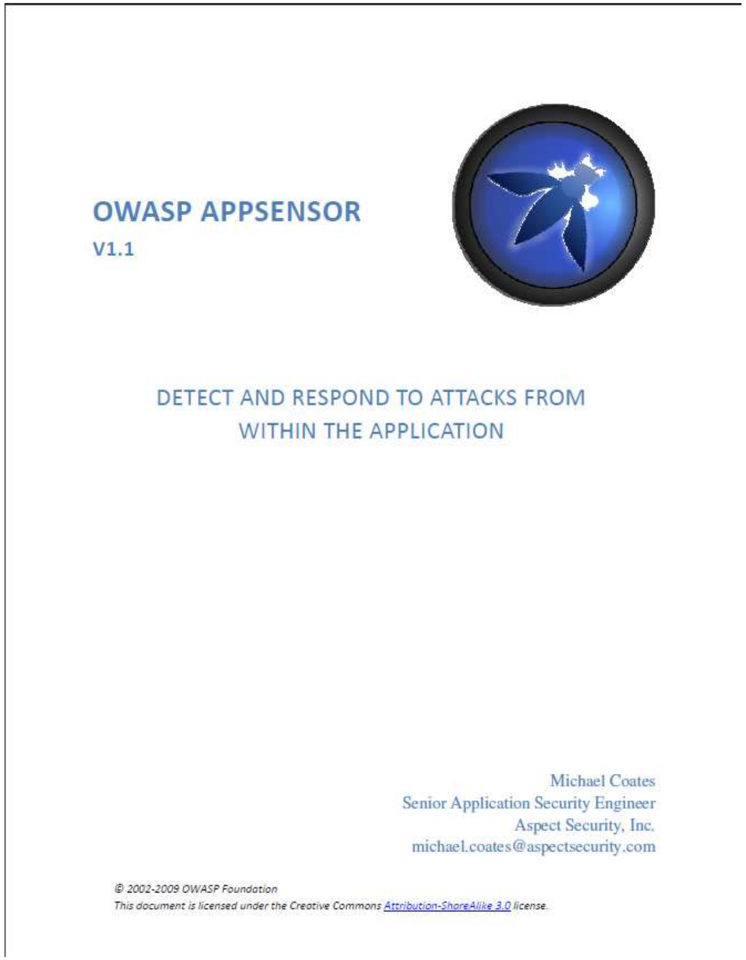
Creative Commons (CC) Attribution Share-Alike
Free version at http://www.owasp.org

- ASD STIG:
  “Ensure a code review is performed before the application is released.”

- Application Security Verification Standard: Defines a standard for conducting both automated and manual application security assessments

http://www.owasp.org/index.php/ASVS

APP6130 – Systems Monitoring



OWASP APPSENSOR

V1.1

DETECT AND RESPOND TO ATTACKS FROM
WITHIN THE APPLICATION

Michael Coates
Senior Application Security Engineer
Aspect Security, Inc.
michael.coates@aspectsecurity.com

- ASD STIG:
  “Ensure…alerts are provided immediately when unusual or inappropriate activity is detected.”

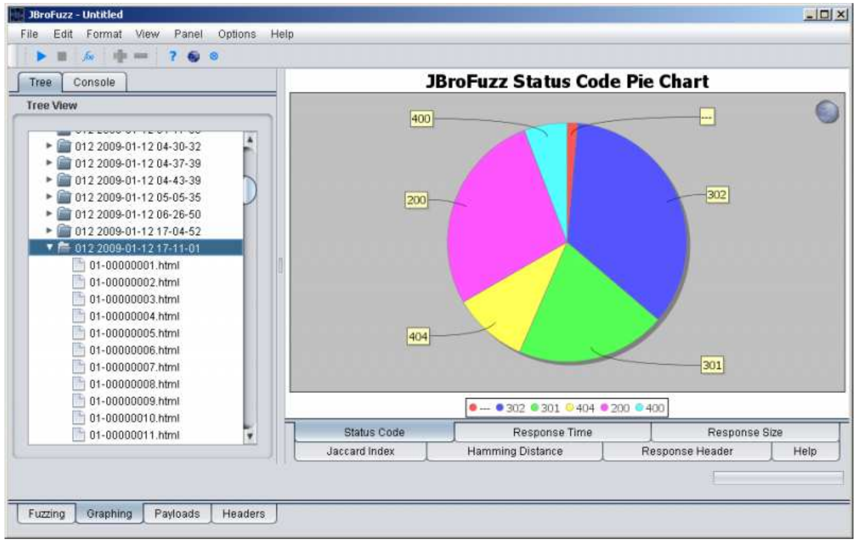
- AppSensor Project:
  Defines a methodology to implement intrusion detection and automated response into an existing application

http://www.owasp.org/index.php/Category:OWASP_AppSensor_Project

APP5100 – Fuzz Testing

- ASD STIG:
  "Ensure fuzz testing is included … and performed for each application…"

- JBroFuzz:
  a web application fuzzer for requests being made over HTTP or HTTPS



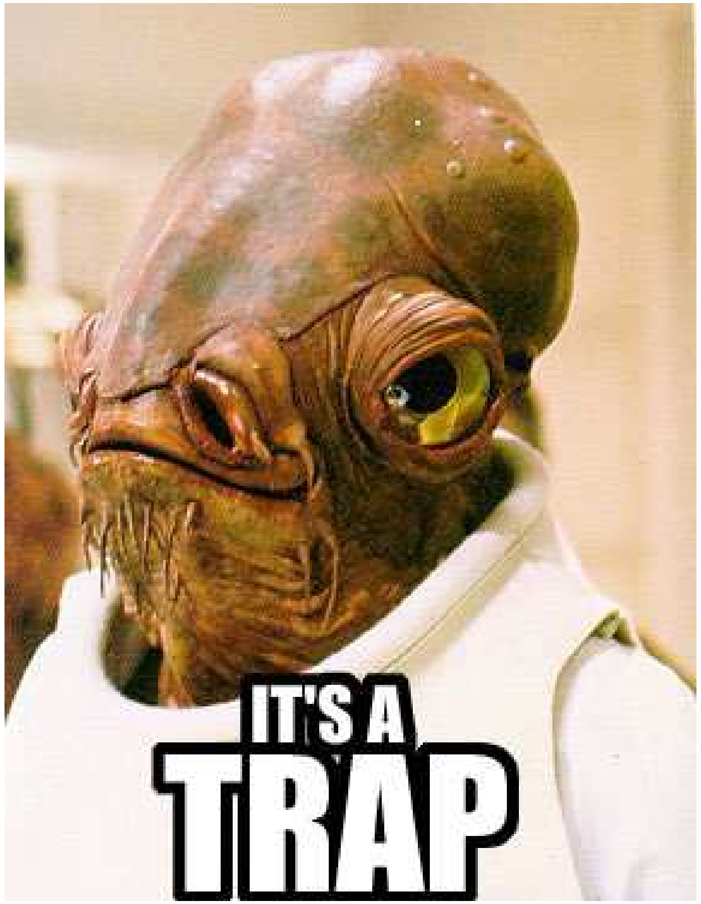
http://www.owasp.org/index.php/Category:OWASP_JBroFuzz
(also included in the OWASP LiveCD)

Other OWASP Projects

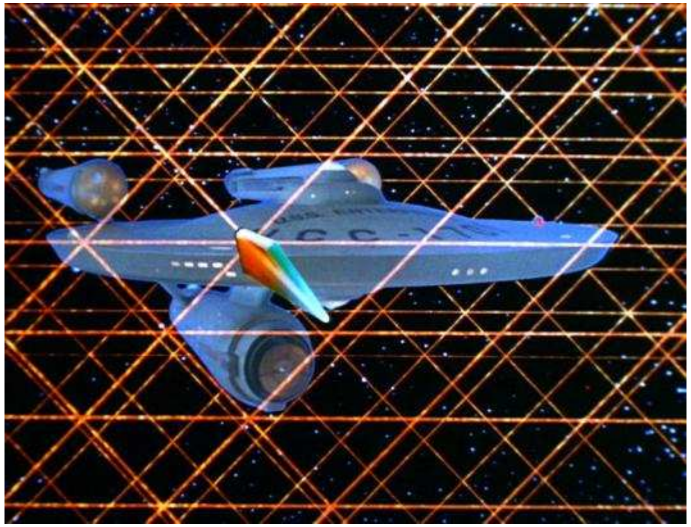
- OWASP ESAPI Project
  - Provides an open source collection of all the application security controls for developers
  - http://www.owasp.org/index.php/ESAPI
- OWASP LiveCD Project
  - A collection of open source security tools for web developers, testers and security professionals
  - http://www.owasp.org/index.php/LiveCD
- OWASP Legal Project
  - Provides contract language for acquiring secure software
  - http://www.owasp.org/index.php/Legal

Top 10 ASD Gimmes

1. APP3270: Identify classification of pages
2. APP3320: Enforce DoD password policy
3. APP3390: Lock users after 3 attempts w/in 1 hr
4. APP3400: Do not allow automatic timed unlock
5. APP3415: Enforce session idle timeout



Top 10 ASD Gimmes (cont.)



6. APP3420: Include a logout link
7. APP3440: Include the DoD Logon banner
8. APP3530: Set charset in the Content-Header
9. APP3610: Don’t use hidden fields
10. APP3660: Show last and failed login details, including date, time and IP address

Summary

- Know the variety of ASD STIG requirements

- Leverage OWASP Projects:
  - http://www.owasp.org/index.php/Category:OWASP_Project

Questions?

Management
Implementation
Verification
Foundation

Contact:

Jason Li

jason.li@aspectsecurity.com

ASPECT SECURITY
Application Security Specialists